Processor Binding Corporate Rules (BCRs), for intra-group transfers of personal data to non EEA countries

Sopra HR Software as a Data Processor

1. INTRODUCTION

As a global outsourcing service and software provider, SOPRA HR SOFTWARE offers a wide range of Human Resources business solutions to its customers such as talent management, payroll services, time and attendance, benefits services, business strategy, and workforce management. When providing outsourcing services, support services or other services to its customers, SOPRA HR SOFTWARE processes large amounts of Personal Data on behalf and under the instructions of its customers, in particular Personal Data relating to its customers' employees. In this context, SOPRA HR SOFTWARE is committed to ensure that adequate safeguards are in place to protect Personal Data pertaining to its customers.

Outsourcing, license & support agreements, outsourcing agreements and service agreements are often entered into for the benefit of a number of customer entities and the services delivered by SOPRA HR SOFTWARE may be sub-contracted to a number of other entities from SOPRA HR SOFTWARE group, some of which may be based outside the EU.

Under the provisions of the European Union Directive 95/46, any transfer of Personal Data outside the European Economic Area (EEA) shall be framed by specific safeguards, with a view to make the use of Personal Data compliant with European Data Protection Principles. Thus, the adoption and the implementation of Processor Binding Corporate Rules (BCRs) within SOPRA HR SOFTWARE will aim to guarantee to SOPRA HR SOFTWARE's customers that intra-group data transfers related to Personal Data outside the European Economic Area (EEA) made in relation with the performance of license & support agreements, outsourcing agreements and service agreements are adequately framed in accordance with the provisions of the 95/46 and 2002/58 EU Directives. Thus, the adoption of Processor BCRs will enable its customers to transfer Personal Data to SOPRA HR SOFTWARE and to its sub-contractors outside of the EU. In addition, it should ease the compliance burden associated with any support services, outsourcing services or other services and could provide a competitive edge to SOPRA HR SOFTWARE when offering this solution.

Beyond, SOPRA HR SOFTWARE and its employees are responsible for protecting and respecting personal information to which they have access. Therefore, we believe that our BCRs are an essential tool to effectively manage this important responsibility and to broadcast and share our culture on Privacy within the group. With regard to the scope of our BCRs, appropriate entities and employees of SOPRA HR SOFTWARE shall comply with the following provisions, as well as with applicable local laws.

At local level, and according to the terms of our BCRs, each Local Data Processor will have to sign a BCRs agreement and shall take every necessary step to ensure compliance with the provisions of the BCRs. Compliance with these provisions and procedures will especially rely on training programs and auditing activities, on a day to day basis.

Because of their wide scope in terms of privacy compliance, the use of BCRs at local level will, without any doubt, facilitate the management of privacy compliance and will help to ensure that local representatives take ownership of data protection.

Would a violation of the BCRs be established, any corrective measures (legal, technical or organizational measures) as well as any appropriate sanction (against the Local Data Processor or, according to local labor law, a local employee) may be taken on the initiative of the Head Processor, the Group Data Privacy Manager, the Local Data Processor or the Local Data Privacy Manager.

Finally, the adoption of Processor BCRs within SOPRA HR SOFTWARE will fit within an ongoing process which has already been implemented in relation with the Controller BCRs to which SOPRA HR SOFTWARE is bound and which were approved by the CNIL, as lead data protection authority, on September 2012. Thus, a large part of the actions and measures which have been carried out according to the pre-existing BCRs will only have to be slightly modified and completed to address the specificities of the Processor BCRs, making the implementation of the new BCRs much easier.

2. DEFINITIONS AND DATA PROTECTION PRINCIPLES

2.1. DEFINITIONS

The terms and expressions used in the BCRs are defined in Appendix 1, provided that these terms and expressions shall always be interpreted according to the EU 95/46 and 2002/58 Directives.

2.2. DATA PROTECTION PRINCIPLES

Within the scope of the BCRs (see paragraph 3), any transfer of Personal Data to a third country which does not ensure an adequate level of protection shall always comply with the data protection principles, defined in specific paragraphs of the BCRs or in Appendix 2, in accordance with the provisions of the EU 95/46 and 2002/58.

3. SCOPE OF THE BCRs

3.1. GEOGRAPHICAL SCOPE

The BCRs shall apply to transfers of Personal Data from entities of SOPRA HR SOFTWARE established within the European Union to other SOPRA HR SOFTWARE entities throughout the world listed in Appendix 3. Appendix 3 gives a list of all SOPRA HR SOFTWARE entities bound by the BCRs.

It is the choice of the Data Controller to apply the BCRs to:

- all Personal Data processed by SOPRA HR SOFTWARE on the Data Controller's behalf and under its instructions and that are submitted to European Union law (for instance, Personal Data that have been transferred from the European Union), or;
- all processing of data processed by SOPRA HR SOFTWARE on the Data Controller's behalf and under its instructions within the group whatever the origin of the Personal Data.

3.2. MATERIAL SCOPE

The nature and purposes of the Personal Data being transferred within the scope of the BCRs is detailed in Appendix 4.

4. EFFECTIVENESS OF THE BCRs

4.1. ACCESS TO BCRs FOR DATA SUBJECT

The BCRs shall always be readily available to every Data Subject and therefore shall be uploaded on SOPRA HR SOFTWARE internet and intranet websites. A Data Subject shall always be able to obtain, upon request, a copy of the BCRs from the Local Data Privacy Manager, the Local Data Processor or the Group Data Privacy Manager.

Furthermore, specific FAQs shall be available for Data Subjects on SOPRA HR SOFTWARE internet websites, with a view to clarify any question Data Subjects may have about the BCRs on any related matter.

4.2. INTERNAL COMPLAINT MECHANISM

SOPRA HR SOFTWARE hereby commits to create a specific contact point for the Data Subjects.

Should SOPRA HR SOFTWARE or any of its entities be aware of a claim or request from a Data Subject who believes that its Personal Data is not processed in accordance with the BCRs or the applicable local law, he shall promptly inform the Data Controller of such claim or request without obligation to handle it, expect if it has been agreed otherwise with the Data Controller.

SOPRA HR SOFTWARE hereby undertakes to handle complaints from Data Subjects where the Data Controller has disappeared factually or has ceased to exist in law or became insolvent.

In all cases where SOPRA HR SOFTWARE handles complaints from Data Subjects, the complaints shall be dealt by a clearly identified local department which benefits from an appropriate level of independence in the exercise of its functions (for instance the local compliance officer or the General counsel). In those cases, specific guidelines and procedures shall be in place within the group, at local level, to ensure a complaint mechanism to be consistent and to ensure sufficient information to be provided to the Data Subjects about these procedures, in particular:

- where to complain;
- in which form;
- the timescale for the reply on the complaint;
- consequences in case of rejection of the complaint;
- consequences in case the complaint is considered as justified;
- consequences if the Data Subject is not satisfied by the replies (right to lodge a claim before the court/Data Protection Authority).

When a complaint is registered, it must be acknowledged and handled within a reasonable period of time (two months). If the SOPRA HR SOFTWARE representatives fail to solve the claim at local level, the complaint handling mechanism shall allow escalating the problem to the Group Data Privacy Manager who shall respond within 2 months. Each Local Data Processor and Local Data Privacy Manager shall regularly report to the Group Data Privacy Manager about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the group, where the complaints may have revealed a "gap" in terms of Privacy compliance.

All SOPRA HR SOFTWARE representatives and employees shall, at local level, do their best efforts to help the Local Data Processor or the Local Data Privacy Manager to settle a complaint (see paragraph 5.3).

Prior to referring a case to the relevant court, each party should make its best efforts to solve a claim through the internal complaint mechanism described above.

4.3. SECURITY AND CONFIDENTIALITY

Ensuring that personal information is appropriately protected from data breaches is a SOPRA HR SOFTWARE top priority (see Appendix 2). Thus:

1. Each Local Data Processor shall process the Personal Data only on behalf of the Data Controller and in compliance with its instructions regarding the data processing and the security and confidentiality measures as provided in the Service Agreement.

2. Each SOPRA HR SOFTWARE employee shall process the Personal Data only on behalf of the SOPRA HR SOFTWARE management and in compliance with its instructions regarding the data processing and the security and confidentiality measures as provided in the Service Agreement with a client.

3. Each Local Data Processor shall implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Consequently, appropriate information security policies and procedures shall be designed and implemented within the group. These security policies set up all appropriate physical and logical measures with a view to prevent or deter accidental destruction, modification or unauthorized disclosure or access to Personal Data. These policies and procedures shall be regularly audited (see paragraph 4.5).

4. Sensitive Data shall be processed with enhanced and specific security measures.

5. Access to Personal Data is limited to Recipients for the sole purpose of performing their professional duties. Disciplinary sanctions may occur if a SOPRA HR SOFTWARE employee fails to comply with the appropriate information security policies and procedures.

Where a Local Data Processor requests that another entity of SOPRA HR SOFTWARE undertakes Processing of Personal Data on its behalf (for a short term period as well as for a long term period, depending on the case), the following safeguards shall be followed:

1. Where the data processing is carried out, the Local Data Processor shall choose a Sub-Processor providing sufficient guarantees in respect of the Technical and Organizational Security Measures governing the processing to be carried out, and must ensure compliance with those measures. The appointed entity of SOPRA HR SOFTWARE shall undertake in writing to provide those sufficient guarantees. Local Data Privacy Managers, in coordination with the Group Data Privacy Manager, shall be able to provide templates of the appropriate clauses to a Local Data Processor within the group.

2. The appointed entity of SOPRA HR SOFTWARE must not process the data except on instructions from the Local Data Processor, unless he is required to do so by law.

3. Upon termination of the work to be done, the appointed entity of SOPRA HR SOFTWARE shall undertake to delete all the data transferred or, if any legal data retention requirement is applicable, to keep it recorded, provided that appropriate technical and organizational measures are taken to protect Personal Data against any unlawful form of processing.

4.4. TRAINING PROGRAMS

Any SOPRA HR SOFTWARE employee who collects, processes or has access to Personal Data shall be provided with specific training programs in order to improve its practical skills and knowledge that relate to data protection issues, especially the BCRs:

1. BCR's and all related guidelines, procedures or policies shall be uploaded on SOPRA HR SOFTWARE corporate intranet and permanently accessible to every employee.

2. Access to the BCRs and all related guidelines, procedures or policies shall be granted to every SOPRA HR SOFTWARE new employee. Internal notices shall also be transmitted within the group to raise awareness on the BCRs.

3. New employees who collect, process or have access to Personal Data shall be required to follow a privacy compliance training program. Furthermore, all employees who collect process or have access to Personal Data shall be required to follow such a program, on a regular basis. All employees must pass a knowledge check following their completion of the training to confirm their knowledge and skills on privacy issues.

4. Employees involved in the development of tools used to process personal data shall also be required to follow a training program, on a regular basis.

5. At local level, each Local Data Processor and/or Local Data Privacy Manager shall feel free to enhance the privacy training programs described above by adding any appropriate training material.

6. Privacy training programs shall be reviewed and approved by experienced SOPRA HR SOFTWARE officers, in coordination with the Local Data Processor, the Local Data Privacy Manager, the Group Data Privacy Manager. Procedures related to privacy training programs shall be regularly audited (see paragraph 4.5).

4.5. AUDIT PROGRAMME

Data Protection audits shall be carried out on a regular basis (subject to more stringent local laws, at least one audit every 3 years) by internal or external accredited audit teams to ensure that the BCRs and all related policies, procedures or guidelines are updated and applied :

1. Data Protection audits shall cover all aspects of the BCRs and all related policies, procedures or guidelines, including methods of insuring that corrective measures will take place. However, the scope of each audit can be strengthened to limited aspects of the BCRs and/or the related policies, procedures or guidelines, including methods of insuring that corrective measures will take place.

2. Data Protection audits shall be decided directly by the Compliance Department or upon specific request of the Head Processor, a Local Data Processor, a Local Data Privacy Manager or the Group Data Privacy Manager. The ones in charge of handling an audit will always benefit from an appropriate level of independence in the exercise of their duties.

3. The results of all audits shall be communicated to the Head Processor (especially to the Head Processor's management), and the Local Data Processor, and/or the Local Data Privacy Manager, and/or the Group Data Privacy Manager but also the results of all audits shall be made accessible to the Data Controller.

4. The Data Protection Authorities competent for the Data Controller shall receive a copy of such audit upon request and have the power to carry out a data protection audit themselves if required and legally possible. Each Local Data Processor shall accept to abide by the advice of a Data Protection Authority on any issue related to the BCRs.

Each Local Data Processor or Sub-processor handling the Personal Data of a particular Data Controller shall accept, at the request of that Data Controller to submit their data processing facilities for audit of the processing activities relating to that Data Controller which shall be carried out by the Data Controller or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Controller, where applicable, in agreement with the Data Protection Authority.

5. As provided by section 3 of paragraph 5.1, Local Data Privacy Managers, in coordination with the Group Data Privacy Manager shall report every year to the Head Processor about all the actions and measures taken with regard to Data Protection issues (training programs, inventory of Personal Data processing implemented, management of complaints, etc.). Furthermore, each local data privacy Manager shall take every necessary step to make sure that Local Data Processors comply with the provisions of the BCRs. To this end, a "BCR compliance check-list" shall be used at local level to make compliance checks.

6. The Group Data Privacy Manager shall also regularly report to the Head Processor about the implementation of the BCRs within each Local Data Processor.

7. Thanks to the audit results and the reports mentioned above, the Head Processor (especially the Head Processor's management), and/or the Group Data Privacy Manager shall decide any appropriate legal, technical or organizational measure in order to improve Data Protection management within the group, both at global and/or local level.

5. BINDINGNESS OF THE BCRs

5.1. COMPLIANCE AND SUPERVISION OF COMPLIANCE

SOPRA HR SOFTWARE commits to appoint, in each entity of SOPRA HR SOFTWARE group, appropriate staff with top management support to oversee and ensure compliance with the rules stated in SOPRA HR SOFTWARE BCR.

At local level, each Local Data Privacy Manager shall be responsible for the implementation of the BCRs. Thus:

1. Each entity of SOPRA HR SOFTWARE shall take every necessary step to make sure that Local Data Processors comply with the provisions of the BCRs. To this end, a "BCR compliance check list" shall be used at local level to make compliance checks. Data Protection audits decided by the Compliance Department or the Group Data Privacy Manager may focus on how these compliance checks are made at local level.

2. Local Data Privacy Managers, in coordination with the Group Data Privacy Manager, shall always be at the disposal of both Local Data Processor and Data Subjects to provide any help with regard to a data protection issue, especially the BCRs.

3. Local Data Privacy Managers, in coordination with the Group Data Privacy Manager, shall report every year to the Head Processor about all the actions and measures taken with regard to Data Protection issues (training programs, inventory of Personal Data processing implemented, management of complaints, etc.), especially the implementation of the BCRs.

4. Each Local Data Processor and Local Data Privacy Manager shall regularly report to the Group Data Privacy Manager about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the group, where the complaints may have revealed a "gap" in terms of Privacy.

5. Local Data Privacy Managers, in coordination with the Group Data Privacy Manager, shall be able to provide any appropriate templates (i.e. notices of information, clauses, etc.) to each Local Data Processor within the group for any purpose related to a data protection issue.

Furthermore, in terms of supervision of compliance, specific measures shall be taken to ensure the right implementation of the BCRs:

1. The Group Data Privacy Manager shall regularly report to the Head Processor about the implementation of the BCRs within each Local Data Processor.

2. Data Protection audits shall be decided directly by the Compliance Department or upon specific request of a Local Data Processor, a Local Data Privacy Manager or the Group Data Privacy Manager. The results of all audits or reports shall be communicated to the Head Processor (especially to the Head Processor's management), and the Local Data Processor, and/or the Local Data Privacy Manager, and/or the Group Data Privacy Manager.

3. Thanks to the audit results and the reports mentioned above, the Head Processor (especially the Head Processor's management), the Group Data Privacy Manager, a Local Data Processor or a Local

Data Privacy Manager shall decide any appropriate measure in order to improve Data Protection management within the Group, both at global and/or local level.

4. If a violation of the BCRs is established, any correction measure (legal, technical or organizational measure) as well as any appropriate sanction (against the Local Data Processor or, according to local labor law, a local employee) may be taken on the initiative of the Head Processor, the Group Data Privacy Manager, a Local Data Processor or a Local Data Privacy Manager.

5. Privacy training programs shall be reviewed and approved by experienced SOPRA HR SOFTWARE officers, in coordination with the Group Data Privacy Manager and Local Data Privacy Managers. Procedures related to privacy training programs shall be regularly audited (see paragraph 4.5).

5.2. THIRD PARTY BENEFICIARY RIGHTS

Specific rights are granted to Data Subjects to enforce the BCRs as third-party beneficiaries only if:

i. the Data Subject is not able to bring a claim against the Data Controller because the Data Controller has factually disappeared or ceased to exist in law or has become insolvent, and

ii. no successor entity has assumed the entire legal obligations of the Data Controller by contract of by operation of law, in which case the Data Subject can enforce its rights against such entity, and

iii. Data Subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCRs.

A Data Subject shall have the right to enforce, as a third party beneficiary, the provisions of the BCRs related to:

- Security and confidentiality principles and the duty to respect the BCRs (see paragraphs 4.3 and 6.1)
- Liability and jurisdiction provisions (see paragraph 5.3)
- Right to complain through the internal complaint mechanism (see paragraph 4.2)
- Cooperation duties with Data Protection Authorities and with each Data controller (see paragraph 5.5 and 5.6)
- Privacy principles according to which SOPRA HR SOFTWARE is bound (see Appendix 2)
- National legislation preventing respect of BCRs (see paragraph 6.3)
- Easy access to BCRs for Data Subjects (see paragraph 4.1) List of all SOPRA HR SOFTWARE entities bound by the BCRs (see paragraph 3 and Appendix 3).

5.3. LIABILITY AND JURISDICTION

1. Liability towards a Data Subject: as stated in article 5.2, specific rights are granted to Data Subjects to enforce the BCRs as third-party beneficiaries only if:

i. the Data Subject is not able to bring a claim against the Data Controller because the Data Controller has factually disappeared or ceased to exist in law or has become insolvent, and

ii. no successor entity has assumed the entire legal obligations of the Data Controller by contract of by operation of law, in which case the Data Subject can enforce its rights against such entity.

iii. Data Subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCRs.

When article 5.2 finds to be applicable, the Data Subjects' rights shall cover the judicial remedies for any breach of the rights guaranteed and the right to receive compensation for any damage (material harm but also any distress) within the delay provided at paragraph 4.2 when applicable.

Data subjects shall be entitled to lodge a complaint before the Date Protection Authority or Courts competent for the EU Controller. If this is not possible for the reasons stated above, the Data Subject may take action before the Data Protection Authority or the court competent for the EU entity of the Processor at the origin of the transfer. If those situations are not applicable, the Data Subjects shall be entitled to lodge a complaint to the court of his place of residence. If more favorable solutions for the Data Subject exist according to national law, then they would be applicable.

The EU exporters processor (e.g. the EU contracting party with the Data Controller) shall accept responsibility for and to agree to take the necessary action to remedy the acts of other members of the BCRs established outside of EU or breaches caused by external Sub-processors established outside of EU and to pay compensation for any damages resulting from the violation of the BCRs. This EU exporters processor will accept liability as if the violation had taken place by him in the member state in which he is based instead of the member of the group outside the EU or the external Sub-processor established outside of EU.

This EU exporter processor may not rely on a breach by a Sub-processor (internal or external of the group) of its obligations in order to avoid its own liabilities.

Liability as between the parties shall be limited to actual damage suffered. Indirect or punitive damages shall be specifically excluded.

2. Liability towards the Data Controller: the BCRs shall be made binding towards the Data Controller. To that end, the BCRs shall be annexed to the Service Agreement signed with the Data Controller or a through a specific reference made to it with a possibility of electronic access.

Where Data Controllers can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCR, the Data Controllers' rights shall cover the judicial remedies and the right to receive compensation.

The EU exporters processor (e.g. the EU contracting party with the Data Controller) shall accept responsibility for and to agree to take the necessary action to remedy the acts of other members of the BCRs established outside of EU or breaches caused by external Sub-processors established outside of EU and to pay compensation for any damages resulting from the violation of the BCRs. This EU exporters processor will accept liability as if the violation had taken place by him in the member state in which he is based instead of the member of the group outside the EU or the external Sub-processor established outside of EU.

This EU exporter processor may not rely on a breach by a Sub-processor (internal or external of the group) of its obligations in order to avoid its own liabilities.

Liability as between the parties shall be limited to actual damage suffered. Indirect or punitive damages shall be specifically excluded.

3. Burden of proof: where Data Subjects or Data Controller can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCRs, it will be for the EU exporters processor to prove that the member of the corporate group outside of Europe or the external Sub-processor was not responsible for the breach of the BCRs giving rise to those damages or that no such breach took place.

If the EU exporters processor can prove that the member of the group outside the EU is not responsible for the act, it may discharge itself from any responsibility.

5.4. SANCTIONS

Would a violation of the BCRs, either by Local Data Processor representatives or employees, be established, any appropriate disciplinary sanction or judicial action may occur, in accordance with local labor law, on the initiative of the Head Processor, the Group Data Privacy Manager, the Local Data Processor or the Local Data Privacy Manager.

Thus, each Local Data Processor and Local Data Privacy Manager shall pay specific attention to any audit results (see paragraph 4.5) establishing non-compliance issues against representatives or employees, especially in case of:

- non compliance with the Data Protection Principles set out in paragraph 2.2 and Appendix 2;
- non compliance with security policies designed to implement appropriate technical and organizational measures to protect Personal Data;
- non compliance with training programs designed to raise employee's awareness on Data Protection issues.

5.5. MUTUAL ASSISTANCE AND COOPERATION WITH DATA PROTECTION AUTHORITIES

All SOPRA HR SOFTWARE entities are committed to a full cooperation with the EEA data protection authorities who have competent jurisdiction for the relevant Data Controller. Thus:

- The relevant Data Protection Authorities shall receive, upon request, an update copy of the BCRs or all related procedures, policies or guidelines;
- The Local Data Processor shall reply within a reasonable period of time to any request addressed by a relevant Data Protection Authority with competent jurisdiction, including audit requests;
- The Local Data Processor shall apply any relevant recommendation or advice from a relevant Data Protection Authority relating to the implementation of the BCRs;
- The Local Data Processor shall abide by a decision of a relevant Data Protection Authority with competent jurisdiction, related to the implementation of the BCRs, against which no further appeal is possible before competent courts;

- The Group Data Privacy Manager shall be at the disposal of the relevant Data Protection Authorities for any matter related to the implementation of the BCRs.

Furthermore, members of SOPRA HR SOFTWARE shall cooperate and assist each other to handle a request or complaint from an individual (see paragraph 4.2) or inquiry by Data Protection Authorities.

5.6. COOPERATION WITH DATA CONTROLLER

All SOPRA HR SOFTWARE entities and their Sub-processors are committed to cooperate and assist the Data Controller to comply with the Applicable Data Protection Law, in a reasonable time and to the extent reasonably possible, in particular in relation with:

- Data Subjects rights: SOPRA HR SOFTWARE and its Sub-processors undertake to cooperate with the Data Controller and help him to meet the legal requirements incumbent on him for the protection of Personal Data, in particular for the exercise of the rights of access, rectification, erasure and blocking of data;
- Handling Data Subjects complaints: SOPRA HR SOFTWARE and its Sub-processors undertake to cooperate with the Data Controller with respect to Data Subjects complaints;
- Data Protection Authorities investigations or inquiries: SOPRA HR SOFTWARE and its Sub-processors undertake to help the Data Controller to be in a position to reply to any investigation or inquiry from the relevant Data Protection Authorities.

6. FINAL PROVISIONS

6.1. RELATIONSHIP BETWEEN NATIONAL LAWS AND THE BCRs

SOPRA HR SOFTWARE undertakes that appropriate entities and employees of SOPRA HR SOFTWARE shall comply with the provisions of the BCRs, as well as with the provisions of the 95/46 and 2002/50 EU Directives and applicable local laws, as provided by article 4 of the 95/46 EU Directive.

Where the local legislation requires a higher level of protection for Personal Data, it always will take precedence over the BCRs.

6.2. ONWARD TRANSFERS TO EXTERNAL PROCESSORS

Where a Local Data Processor requests that a non-SOPRA HR SOFTWARE entity undertakes sub-Processing of Personal Data, the following safeguards shall be followed (see Appendix 2):

1. Where the member of BCRs subcontracts its obligations under the Service Agreement to an external Sub-Processor located in the EEA or in a country recognised by the EU Commission as ensuring an adequate level of protection, it shall be bound by a written agreement stipulating that the Sub-Processor shall act only on instructions from the Local Data Processor and shall be responsible for

the implementation of the adequate security and confidentiality measures (see paragraph 4.3). Local Data Privacy Managers, in coordination with the Group Data Privacy Manager, shall be able to provide templates of the appropriate clauses to a Local Data Processor within the group.

2. Where the member of BCRs subcontracts its obligations under the Service Agreement to an external Sub-Processor located outside of the EEA, with the consent of the Data Controller, it shall do so only by way of a written agreement with the Sub-Processor which provided that adequate protection is provided according to Articles 16, 17, 25 and 26 of the Directive 95/46/EC and which ensure that the external Sub-processor will have to respect the same obligations as are imposed on the member of the BCRs according to the Service Agreement and sections 5.2, 5.3, 5.4, 5.5, 5.6 and Appendix 2 of the BCRs.

6.3. ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRs

Shall a Local Data Processor have reasons to believe that the legislation applicable to him prevents the company from fulfilling the instructions received from the Data Controller or its obligations under the BCRs or service agreement and has substantial effect on the guarantees provided by the rules, he will promptly inform the Data Controller which is entitled to suspend the transfer of data and/or terminate the contract, the Group Data Privacy Manager and the Data Protection Authority competent for the Data Controller.

Where there shall be conflict between national law and the commitments in the BCRs, the Local Data Privacy Manager and the Local Data Processor, in coordination with the Group Data Privacy Manager, shall take a responsible decision on what action to take and will consult the competent Data Protection Authorities in case of doubt.

SOPRA HR SOFTWARE undertakes that it will promptly notify the Data controller about any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. In any case, the request for disclosure should be put on hold and the Data Protection Authority competent for the Data Controller and the lead Data Protection Authority for the BCRs should be clearly informed about it.

6.4. UPDATES OF THE BCRs

In case of, for instance, changes in laws or SOPRA HR SOFTWARE procedures, the terms of the BCRs may be updated on the initiative of the Head Processor, in coordination with the Group Data Privacy Manager. Where a change affects the processing conditions, SOPRA HR SOFTWARE undertakes to inform the Data Controller in such a timely fashion that the Data Controller has the possibility to object to the change or to terminate the service agreement before the modification is made.

Any substantial or non substantial update of the BCRs shall be recorded and kept by the Group Data Privacy Manager who shall provide the necessary information systematically to the Data Controller and upon request to Data Protection Authorities. The Group Data Privacy Manager keeps as well a fully updated list of the members of the group and of the Sub-processors involved in the data processing activities for the Data Controller which shall be made accessible to the Data Controller, Data subjects and Data Protection Authorities.

Any substantial or non substantial update will lead to the communication, to each entity of SOPRA HR SOFTWARE, of an updated version of the BCRs for signature purpose.

SOPRA HR SOFTWARE undertakes that appropriate information will be given, once a year, the appropriate Local Data Processors and the competent Data Protection Authorities about any substantial update.

No transfer shall be made to a new SOPRA HR SOFTWARE entity until this new entity is effectively bound by the BCR and can deliver compliance.

6.5. APPLICABLE LAW / JURISDICTION / TERMINATION / INTERPRETATION OF TERMS

The BCRs shall be adopted by the Head Processor, in coordination with the Group Data Privacy Manager.

The BCRs shall take effect on the date when each entity of SOPRA HR SOFTWARE signs this BCRs agreement and, as a consequence, is legally bound. Each entity of SOPRA HR SOFTWARE recognizes to be bound by the BCRs, from the date of signature of the BCRs agreement and without any other formalities, with respect to other SOPRA HR SOFTWARE entities already bound or about to be bound from the date of their signature, notwithstanding the date and place of signature of a BCRs agreement by each other entity of SOPRA HR SOFTWARE involved, and provided that the terms of the BCRs are strictly identical between each other. Except if an entity of SOPRA HR SOFTWARE is able to prove that the signed BCRs agreement is not strictly identical to the ones signed by other entities, it expressly and irrevocably disclaims challenging the evidence that it is bound by the terms of the BCRs.

In the event that a Local Data Processor would be found in substantial or persistent breach of the terms of the BCRs, the Head Processor may temporarily suspend the transfer of Personal Data until the breach is repaired and shall inform the Data Controller of such a suspension. Should the breach not be repaired in due times, the Head Processor shall take the initiative to terminate the BCRs Agreement and shall inform the Data Controller of such a termination. In such a case, the Local Data Processor shall take every necessary step in order to respect the European rules on transborder data flows (Articles 25-26 of the 95/46 EU Directive), for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission.

The provisions of the BCRs shall be governed by the law of the EEA Member State in which the Local Data Exporter is located.

In accordance with paragraph 5.3claims brought by Data Subjects should be lodged before the court competent for the Data Controller, and if not possible, before the court of the Local Data Exporter.

In case of contradiction between the BCRs and the appendixes, the BCR shall always prevail. In case of contradiction between the BCRs and other global or local policies, procedures or guidelines, the BCR shall always prevail. In case of contradiction or inconsistency, the terms of the BCRs shall always be interpreted and governed by the provisions of the 95/46 and 2002/58 EU Directives.

7. APPENDIXES

Appendix 1 - Definitions

Appendix 2 - Data Protection Principles

Appendix 3 - List of SOPRA HR SOFTWARE entities bound by the BCRs

Appendix 4 - Nature and purposes of the Personal Data being transferred within the scope of the BCRs

Appendix 5 - Model clauses to be included in the service agreement

APPENDIX 1: DEFINITIONS

The terms and expressions used in the BCRs are defined in this appendix, provided that these terms and expressions shall always be interpreted according to the EU 95/46 and 2002/58 Directives.

"**Data Controller**" shall mean any SOPRA HR SOFTWARE customer which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

"**SOPRA HR SOFTWARE**" shall mean SOPRA HR SOFTWARE itself and/or any corporate entity of SOPRA HR SOFTWARE hold, directly or indirectly, by SOPRA HR SOFTWARE, according to article L. 233-3 of the French Commercial Code.

"**Head Processor**" shall mean SOPRA HR SOFTWARE Headquarters located in France which processes Personal Data on behalf of the Data Controller and which is in charge of the formal adoption of BCRs to be implemented within SOPRA HR SOFTWARE.

"**Local Data Processor**" shall mean the legal entity of SOPRA HR SOFTWARE which processes Personal Data on behalf of the Data Controller.

"**Local Data Exporter**" shall mean the legal entity of SOPRA HR SOFTWARE located within the EEA which transfers the Personal Data outside the EEA.

"**Local Data Importer**" shall mean the legal entity of SOPRA HR SOFTWARE located outside the EEA which agrees to receive from the Local Data Exporter Personal Data for further Processing.

"**Local Data Privacy Manager**" shall mean an experienced SOPRA HR SOFTWARE officer within a Local Data Processor who is responsible for managing business awareness and compliance with Applicable Data Protection Law and SOPRA HR SOFTWARE privacy policies, procedures and guidelines, especially the BCRs.

"**Group Data Privacy Manager**" shall mean the senior level manager who is responsible, within the group at Global level, for managing business awareness and compliance with Applicable Data Protection Law and SOPRA HR SOFTWARE privacy policies, procedures and guidelines, especially the BCRs.

"**Directive**" means the European Union Directive number 95/46/EC entitled 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data.

"**Personal Data**": shall mean any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"**Processing of Personal Data**" shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Recipient**" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as Recipients.

"**Sensitive Data**" shall mean Personal Data revealing directly or indirectly the racial or ethnic origin, political, philosophical or religious opinions, trade union affiliation, or related to the health or sexual life of individuals.

"**Sub-Processor**" shall mean any legal entity of SOPRA HR SOFTWARE and member of the BCRs (also called "internal Sub-processor") which processes Personal Data on behalf of the Head Processor or Local Data Processor. When the Sub-processor is not a member of the BCRs, it shall be called "External Sub-Processor".

"**Third Party**" shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, the Data Controller, the Processor and the persons who, under the direct authority of the Processor or the Processor, are authorized to process the data.

"**The Data Subject's Consent**" shall mean any freely given specific and informed indication of his wishes by which the Data Subject signifies his agreement to Personal Data relating to him being processed.

"**Applicable Data Protection Law**" shall mean the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data applicable to a data Processor in the EEA Member State in which the Local Data Exporter is established.

"**Technical and Organizational Security Measures**" shall mean measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

APPENDIX 2: DATA PROTECTION PRINCIPLES

Within the scope of the BCRs, any transfer of Personal Data to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles, set out by the EU Directive 95/46.

TRANSPARANCY AND FAIRNESS

All SOPRA HR SOFTWARE entities and their Sub-processors shall help and assist the Data Controller to comply with the law and undertake to be transparent about sub-processor activities in order to allow the Data Controller to correctly inform the Data Subjects about the following:

a. the identity of the controller and of his representative, if any, and, when appropriate, the place in which the Local Data Importer is based outside the EEA;

b. the purposes of the processing for which the data are intended, and, when appropriate, the purpose(s) of the transfer(s) outside the EEA;

c. any further information such as:

- the categories of data concerned;
- the Recipients or categories of Recipients of the data;
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- the existence of the right of access to and the right to rectify the data concerning him.

PURPOSE LIMITATION

All SOPRA HR SOFTWARE entities and their Sub-processors undertake to process the Personal Data only on behalf of the Data Controller and in compliance with its instructions. If they cannot provide such compliance for whatever reasons, they agree to inform promptly the Data controller of their inability to comply, in which case the Data Controller is entitled to suspend the transfer of data and/or terminate the service agreement.

On the termination of the provision of the data processing services, SOPRA HR SOFTWARE entities and their Sub-processors shall, at the choice of the Data Controller, return all the Personal Data transferred and the copies thereof to the Data Controller or shall destroy all the Personal Data and certify to the Data Controller that it has done so, unless legislation imposed upon them prevents it from returning or destroying all or part of the Personal Data transferred. In that case, SOPRA HR SOFTWARE entities and their Sub-processors shall inform the Data Controller and warrant that they shall guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

DATA QUALITY AND PROPORTIONALITY

All SOPRA HR SOFTWARE entities and their Sub-processors shall help and assist the controller to comply with the Applicable Data Protection Law, in particular:

- All SOPRA HR SOFTWARE entities and their Sub-processors shall execute any necessary measures when asked by the Data Controller, in order to have the data updated, corrected or deleted. They shall inform each member to whom the data have been disclosed of any rectification, or deletion of data.
- All SOPRA HR SOFTWARE entities and their Sub-processors shall execute any necessary measures when asked by the Data Controller, in order to have the data deleted or anonymised from the moment the identification form is not necessary anymore. SOPRA HR SOFTWARE and its Sub-processors shall communicate to each entity to whom the data have been disclosed of any deletion or anonymisation of data.

SECURITY

All SOPRA HR SOFTWARE entities and their Sub-processors shall comply with the security and organizational measures which at least meet the requirements of the Data Controller's Applicable Data Protection Law and any existing particular measures specified in the service agreement.

SOPRA HR SOFTWARE and its Sub-processors are committed to immediately inform the Data Controller of any security breach.

DATA SUBJECT RIGHTS

All SOPRA HR SOFTWARE entities and their Sub-processors shall execute any necessary measures when asked by the Data Controller, and communicate any useful information in order to help the Data Controller to comply with the duty to respect the rights of the data subjects.

All SOPRA HR SOFTWARE entities and their Sub-processors will transmit to the Data Controller any request received from the Data Subjects without responding to that request, unless he is authorized to do so.

SOPRA HR SOFTWARE shall not sub-contract any of its rights or obligations without the prior written consent of the Data Controller. The Service Agreement shall specify if a general prior consent given at the beginning of the service would be sufficient or if specific consent will be required for each new sub-processing. If a general consent is given, the Data Controller should be informed on any intended changes concerning the addition or replacement of subcontractors in such a timely fashion that the Data Controller has the possibility to object to the change or to terminate the service agreement before the data are communicated to the new sub-processor.

ONWARD TRANSFERS TO EXTERNAL SUB-PROCESSORS

Data may be sub-processed by non-members of the BCRs only where the prior information to the Data Controller and its prior written consent is given. If a general consent is given, the Data Controller should be informed on any intended changes concerning the addition or replacement of subcontractors in such a timely fashion that the Data Controller has the possibility to object to the change or to terminate the service agreement before the data are communicated to the new Sub-processor.

Where SOPRA HR SOFTWARE subcontracts its obligations under the service agreement, with the consent of the Data Controller, it shall do so only by way of a written agreement with the Sub-processor which provided that adequate protection is provided according to Articles 16, 17, 25 and 26 of the Directive 95/46/EC and which ensure that the external Sub-processor will have to respect the same obligations as are imposed on SOPRA HR SOFTWARE according to the service agreement and sections of the BCRs..

APPENDIX 3: LIST OF THE SOPRA HR SOFTWARE ENTITIES BOUND BY THE BCRs

1. Local SOPRA HR SOFTWARE entities located within the EEA

WORLD

HEAD PROCESSOR	Sopra HR Software SAS
Form	Société par Actions Simplifiée
Registered address	PAE Les Glaisins 74940 Annecy-le-Vieux France
TVA communautaire	FR61519319651
Legal representative	Edgard DAHDAH
Group Data Privacy Manager	Eric Miroglio
Local Data Privacy Manager	Eric Miroglio

EUROPE

LOCAL DATA PROCESSOR	Sopra HR Software Limited
Form	Limited Liability
Registered address	30 Old Broad Street London EC2M 1RX United Kingdom
Local Data Privacy Manager	Alan Brennan

LOCAL DATA PROCESSOR	Sopra HR Software SPRL
Form	BVBA
Registered address	Avenue Louise 326 boîte 29 1050 Bruxelles Belgium
Local Data Privacy Manager	Julia Mateffi

LOCAL DATA PROCESSOR	Sopra HR Software SARL
Form	SARL
Registered address	8308 Capellen 89 E, Parc d'activités, Capellen Luxembourg
Local Data Privacy Manager	Julia Mateffi

LOCAL DATA PROCESSOR	Sopra HR Software GmbH
Form	GmbH
Registered address	Valoisplatz 2 26382 Wilhelmshaven Germany
Local Data Privacy Manager	Enno Beening

LOCAL DATA PROCESSOR	Sopra HR Software SRL
Form	SRL
Registered address	Assago, Strada Palazzo A7 4 cap 20090, frazione Milanofiori Italy
Local Data Privacy Manager	Thierry Reydet

LOCAL DATA PROCESSOR	Sopra HR Software SLU
Form	Limited Liability
Registered address	Avenida de Manoteras 48 Planta 1 – Edificio B 28050 Madrid Spain
Local Data Privacy Manager	Thierry Reydet

2. Local SOPRA HR SOFTWARE entities located outside the EEA

EUROPE

LOCAL DATA PROCESSOR	Sopra HR Software SaRL
Form	société à responsabilité limitée
Registered address	18 avenue Louis Casaï 1209 Genève Switzerland
Local Data Privacy Manager	Eric Miroglio

AFRICA

LOCAL DATA PROCESSOR	Sopra HR Software SaRL
Form	SUARL société unipersonnelle à responsabilité limitée
Registered address	92, bd Anfa, Etage 6 20100 Casablanca Morocco
Local Data Privacy Manager	Zied Mokni

LOCAL DATA PROCESSOR	Sopra HR Software SaRL
Form	SARL société à responsabilité limité
Registered address	Immeuble Tunimara Rue du Lac Constance 1053 Les Berges du Lac Tunisia
Local Data Privacy Manager	Zied Mokni

APPENDIX 4: NATURE AND PURPOSES OF PERSONAL DATA BEING TRANFERRED WITHIN THE SCOPE OF THE BCRS

Purposes	Nature of the data transferred
Maintenance support and/or AMS activities - change order and analysis - production migration validation - document business requirements and participation in tests - user test systems fixes/enhancements and procedure changes - research systems and operational issues and determine root cause, fix, or temporary workaround - execute ad-hoc queries in support of problem resolution - assist with testing, validation and data loading - interaction with HRA via email or phone	- Customer Employees (full time and part time) - Retired Employees of Customer - Job Candidates of Customer • *Employee demographics (age, date and place of birth, personal identity, personal address);* • *Payroll information* • *Statutory / contracts information* • *Financial Information (bank account details)*
Outsourcing MPS (Managed Payroll Services): - Payroll file processing: production of payroll files - Direct deposit: establish direct deposit for employees, modify and/or delete employee direct deposit details as requested - Tax changes: maintain and update employee's tax Information - Status update call: updates on status of request with HRA - Research and resolution: research various payroll discrepancies as a result of errors, work with HRA to resolve the same	Customer Employees (full time and part time) - Retired Employees of Customer - Job Candidates of Customer • *Employee demographics (age, date and place of birth, personal identity, personal address);* • *Payroll information* • *Statutory / contracts information* *Financial Information (bank account details)*

Purposes	Nature of the data transferred
Outsourcing PPO (Payroll Processing Outsourcing) - Manual entry update or processing of Personal Data - Monitor all scheduled inbound interfaces prior to payroll processing and validate the same for accuracy and completeness, review various reports as part of post payroll validation - Update records of employees regarding holiday leave - New employee setup procedure - Add, modify or delete payroll-related information	Customer Employees (full time and part time) - Retired Employees of Customer - Job Candidates of Customer • *Employee demographics (age, date and place of birth, personal identity, personal address);* • *Payroll information* • *Statutory / contracts information* *Financial Information (bank account details)*

APPENDIX 5: MODEL DATA PROTECTION CLAUSES TO BE USED IN SERVICE AGREEMENTS SIGNED WITH CUSTOMERS

HRAS (hereinafter the "Service Provider") will be required, for the proper performance of the agreement entered into between the Customer and the Service Provider (hereinafter the "Agreement"), to process on behalf of the Customer, Personal Data[1] relating to persons and other Customer's employee or manager (in particular technical and sales contacts) including without limitation information such as name, address or office phone numbers, wage processing information and, more generally, information concerning human resources management in compliance with the applicable data protection laws and regulations. These Personal Data shall be collected from the Customer. The Customer authorizes the Service Provider to process such Personal Data as it is necessary for the purposes of the Agreement.

Both parties shall be bound by the Binding Corporate Rules (BCRs) which can be made accessible to the Customer upon request with a possibility of electronic access.

It is the decision of the Customer to apply the BCRs to:

- Option 1: all Personal Data processed by the Service Provider on the Data Controller's behalf and under its instructions and that are submitted to European Union law (for instance, Personal Data that have been transferred from the European Union), or;
- Option 2: all processing of data processed by the Service Provider on the Data Controller's behalf and under its instructions within the group whatever the origin of the data.

1.1 Data Controller

The Customer shall remain the Data Controller[2] of the Personal Data processed by the Service Provider under the present Agreement. The Customer shall accomplish the notification formalities concerning the Processing[3] to the relevant data protection authority as determined under the applicable data protection law. As such, the Customer shall determine alone the categories of the Personal Data which are processed, the purposes for which they are processed by the Service Provider and the recipients or type of recipients of such Data Processing. The Customer shall also inform the persons whose Personal Data are processed (hereinafter the "Data Subjects") about the Processing and, when appropriate, obtain their consent, when it is prescribed by the applicable laws. The Customer hereby commits that he is entitled to transfer the Personal Data to the Service Provider in the framework of the present Agreement, that he has obtained the required authorizations and that he complies with the applicable Data Protection legislation.

*[1] "**Personal Data**" means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration. It includes without limitation electronic Data and paper-based files that contain information such as name, home address, office address, e-mail address, age, gender, family information, profession, education, professional affiliations, salary and credit card numbers*

*[2] "**Data Controller**" means, unless expressly designated by legislative or regulatory provisions relating to this processing, a person, public authority, department or any other organization who determines the purposes and means of the data processing*

*[3] "**Process / Processing**" means any operation or set of operations in relation to such data, whatever the mechanism used especially the obtaining, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction*

The Customer shall take all useful precautions, with regard to the nature of the Personal Data and the risks of the Processing, to preserve the security of the Personal Data and, in particular, prevent their alteration and damage, or access by non-authorized third parties.

The Customer shall commit that if the Transfer[4] involves special categories of Personal Data, the Data Subjects have been informed or will be informed before their data being transferred to a third country not providing adequate protection.

The Customer shall also commit to inform the Data Subjects about the existence of Data Processors based outside the EU and of the BCRs. Upon request, the Customer shall make available to the Data Subjects upon request a copy of the BCRs and of the Agreement excluding any sensitive and confidential commercial information.

The Service Provider disclaims and shall not have any liability and responsibility in relation to any violation or breach by the Customer of applicable data protection laws and regulations.

1.2 Data Processor of the Personal Data

The Service Provider shall act as Data Processor and only Process such Data on behalf of and according to the instructions given by Customer in relation to the processing of Personal Data for the provisions of the Services. The Service Provider shall not use or otherwise transfer any Personal Data without the Customer's consent for different purposes than purposes set out in the present Agreement. Service Provider shall Process the Customer Data only on instructions and on behalf of Customer and the Customer hereby allows the Service Provider to process the Personal Data only as directly required for the performance of the Agreement. The Service Provider shall retain the Personal Data according to the Customer's instructions and shall update, correct and/or delete any Personal Data upon the Customer request.

The Service Provider shall undertake to keep the Personal Data in accordance with security requirements that apply within SOPRA HR SOFTWARE providing the technical and organizational security measures in order to protect the Customer's Personal Data against any accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. The Service Provider shall inform the Customer, in writing, to obtain its consent (which cannot be unreasonably withheld) of any substantial change in relation to the prescribed security measures. If the Customer is subject to specific security requirements pursuant to the applicable Data Protection Law, the Customer shall give the Service Provider specific instructions regarding security and the Parties shall agree upon the implementation methods of such instructions. The Service Provider shall be able to use and communicate the Personal Data to its Affiliates, its service providers or sub-contractors as necessary within the performance of the Agreement.

The Service Provider shall promptly notify Customer about (1) any legally binding request for Disclosure of Customer Data by a law enforcement authority unless otherwise prohibited by the

[4] ***"Transfer"*** *means the Disclosure of Personal Data carried out by any person other than the Data Subject. This includes the Disclosure to other SOPRA HR SOFTWARE affiliates and to third parties outside of the SOPRA HR SOFTWARE group of companies*

applicable laws; (2) any Security Breach[5] concerning Customer Data (especially accidental or unauthorized access to Personal Data) that it would be aware of and (3) any request received directly from Customer employees prior to responding to the employee without prior written Customer's consent.

If the Service Provider has reasons to believe that the existing or future legislation applicable to it prevents it from fulfilling the instructions received from the Customer, it shall undertake to promptly notify the Customer which shall be entitled to suspend the transfer of Personal Data and/or terminate the Agreement.

Upon termination of the provision of data processing services, the Service Provider shall, at the choice of the Customer, return all the Personal Data transferred and the copies thereof to the Customer or shall destroy all the Personal Data and certify to the Customer that it has done so, unless legislation imposed them prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the Service Provider will inform the Customer and warrant that it will guarantee the confidentiality of the Personal Data transferred and will no longer actively process the Personal Data.

1.3 Transfer of Personal Data outside of the European Union

The Service Provider may use and provide such Personal Data to any of its Affiliates or subcontractors if it is necessary for the performance of the Agreement. In particular, the Service Provider may transfer such Personal Data to any countries in the European Economic Area where it, any of its Affiliates or subcontractors may do business. The Customer acknowledges that the contractual obligations under the Agreement may be performed particularly by the Affiliates and subcontractors listed in Clause [ ] above.

1.3.1 Sub-processing within the group of the Service Provider (hereafter the "Group"): the Customer hereby authorizes the Service Provider to have the Personal Data sub-processed by sub-contractors who are members of its Group and of the BCRs. The Service Provider undertakes to inform the Customer on any intended changes concerning the addition or replacement of subcontractors in such a timely fashion that the Customer has the possibility to object to the change or to terminate the Agreement for convenience before Personal Data being communicated to the new sub-processor under the conditions stipulated by clause 1.5 herein.

1.3.2 Onward transfers to external sub-processors: the Customer hereby authorizes the Service Provider to have the Personal Data sub-processed by sub-contractors who are not members of its Group as listed in Appendix 1 of this document which can be amended from time to time in order to inform the Customer on any intended changes concerning the addition or replacement of subcontractors in order to enable the Customer to have the possibility to object to the change or to terminate the Agreement

[5] ***Security Breach****" means any information relating (a) the loss or misuse of Personal Data, (b) the accidental, unauthorized and/or unlawful access or handling of Personal Data, or (c) any other act or omission that compromises the security, confidentiality and/or integrity of Personal Data. Data Security Breaches include, among other things, the loss of paper files and portable devices, such as laptops and CDs, containing Personal Data.*

for convenience before Personal Data being communicated to the new sub-processor under the conditions stipulated by the Termination clause 1.6 herein .

If the Service Provider subcontracts its obligations to an external sub-processor located outside the EU, it shall do so only by way of a written agreement with such sub-processor which ensures that adequate protection is provided according to Articles 16, 17, 25 and 26 of the Directive 95/46/EC and also ensures that the external sub-processor shall respect the same obligations as are imposed on the members of the BCRs according to the Agreement and sections 5.2, 5.3, 5.4, 5.5, 5.6 and Appendix 2 of the BCRs. The Customer hereby authorizes the Service Provider to sign, in the Customer name and on its behalf, with the sub-contractor the "standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council" (Commission decision dated February 5, 2010 2010/87/EU).

The Service Provider, as a party of the standard contractual clauses, shall undertake to audit and verify the data processing facilities carried out by the external sub-contractor in the Customer name and on its behalf. Parties hereby agree that the Customer reserves the right to audit and inspect the sub-contractor's data processing activities.

1.4 Rights of Data Subjects to access, rectify, or to object to the Data Processing

In compliance with the French Data protection Law, the employees or executives of the Client are granted of access, rectification and opposition (on legitimate grounds rights) concerning their Personal Data.

All SOPRA HR SOFTWARE entities and their Sub-processors will transmit to the Data Controller any request received from the Data Subjects without responding to that request, unless he is authorized to do so. The access, rectification and opposition (on legitimate grounds rights) rights concerning their Personal Data can be exercised by sending a letter to Sopra HR Software PAE Les Glaisins – 74940 Annecy-le-Vieux – France with a copy of an Identify Document or by sending an email to the local Data Privacy Officer of Sopra HR Software at the following address: acces-cnil@soprahr.com.

The Customer shall undertake to inform its employees or its executives of the methods of exercises of their rights of access, rectification and opposition, according to the Agreement. Service Provider shall comply with Customer's instructions with regards to responding to inquiries from Data Subjects relating to the processing of their Personal Data.

1.5 Customer's audit rights of the data processing facilities

The Service Provider shall accept, at the request of the Customer, to submit their data processing facilities for audit of the processing activities relating to the Customer which shall be carried out by the Customer, or by a third party selected by the Customer which shall be an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data controller, where applicable, in agreement with the applicable DPA.

[The other conditions provided by the audit section of the Agreement shall also apply].

1.6 Termination by the Customer

Where the Customer is informed of a change to Personal Data Processing that affects the processing conditions outside EEA, in particular in case of the addition or replacement of subcontractors by the Service Provider, the Customer shall have the possibility to terminate, without penalty, the Agreement within 30 days from the notification date. Upon termination by the Customer, SOPRA HR SOFTWARE agrees to provide the processing services under former processing conditions or from EEA countries only for a maximum duration of six (6) month.